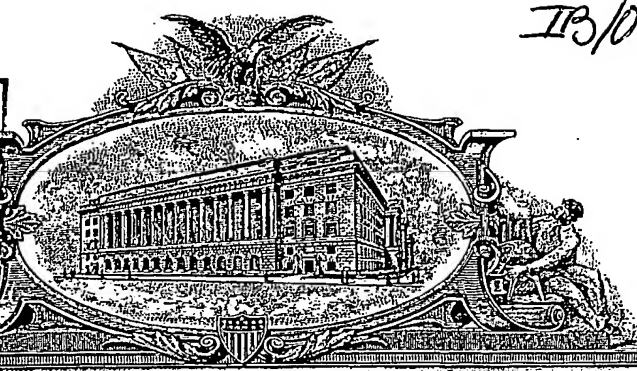


IP/05/00828

REC'D 15 APR 2005  
WIPO PCT

PA 1301562



# THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

April 01, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

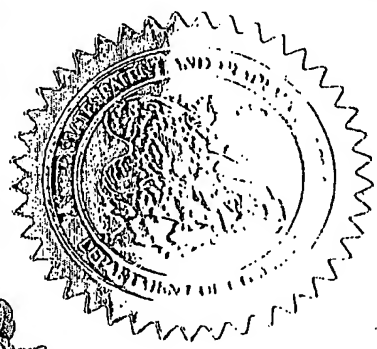
APPLICATION NUMBER: 10/823,378 ✓

FILING DATE: April 12, 2004 ✓

## PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

By Authority of the  
COMMISSIONER OF PATENTS AND TRADEMARKS



*L. Edelen*

L. EDELEN  
Certifying Officer

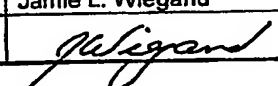
14230 U.S. PTO

PTO/SB/05 (08-03)

Approved for use through 07/31/2008. OMB 0851-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>UTILITY PATENT APPLICATION TRANSMITTAL</b> <small>(Only for new nonprovisional applications under 37 CFR 1.53(b))</small>		<b>Attorney Docket No.</b> 08212/0200353-US0 <b>First Inventor</b> Adam Cain <b>Title</b> SYSTEM AND METHOD FOR ENABLING AUTHORIZATION OF A NETWORK DEVICE USING ATTRIBUTE CERTIFICATES <b>Express Mail Label No.</b> EV398895255US	
<b>APPLICATION ELEMENTS</b> <small>See MPEP chapter 600 concerning utility patent application contents.</small>		<b>ADDRESS TO:</b> MS Patent Application Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450	
1. <input checked="" type="checkbox"/> Fee Transmittal Form (e.g., PTO/SB/17) <small>(Submit an original, and a duplicate for fee processing)</small> 2. <input type="checkbox"/> Applicant claims small entity status. <small>See 37 CFR 1.27.</small> 3. <input checked="" type="checkbox"/> Specification <span style="float: right;">[Total Pages 17]</span> <small>(preferred arrangement set forth below)</small> - Descriptive title of the invention - Cross Reference to Related Applications - Statement Regarding Fed sponsored R & D - Reference to sequence listing, a table, or a computer program listing appendix - Background of the invention - Brief Summary of the invention - Brief Description of the Drawings (if filed) - Detailed Description - Claim(s) - Abstract of the Disclosure 4. <input checked="" type="checkbox"/> Drawing(s) (35 U.S.C. 113) <span style="float: right;">[Total Sheets 6]</span> 5. Oath or Declaration <span style="float: right;">[Total Sheets 5]</span> a. <input checked="" type="checkbox"/> Newly executed (original or copy) b. <input type="checkbox"/> Copy from a prior application (37 CFR 1.63(d)) <small>(for continuation/divisional with Box 18 completed)</small> I <input type="checkbox"/> <b>DELETION OF INVENTOR(S)</b> <small>Signed statement attached deleting inventor(s)          named in the prior application,          see 37 CFR 1.63(d)(2) and 1.33(b).</small> 6. <input checked="" type="checkbox"/> Application Data Sheet. See 37 CFR 1.76		7. <input type="checkbox"/> CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix) 8. Nucleotide and/or Amino Acid Sequence Submission <small>(if applicable, all necessary)</small> a. <input type="checkbox"/> Computer Readable Form (CRF) b. Specification Sequence Listing on: I. <input type="checkbox"/> CD-ROM or CD-R (2 copies); or II. <input type="checkbox"/> Paper c. <input type="checkbox"/> Statements verifying identity of above copies <b>ACCOMPANYING APPLICATION PARTS</b> 9. <input checked="" type="checkbox"/> Assignment Papers (cover sheet & document(s)) 10. <input type="checkbox"/> 37 CFR 3.73(b) Statement <input type="checkbox"/> Power of <small>(when there is an assignee)</small> Attorney 11. <input type="checkbox"/> English Translation Document (if applicable) 12. <input type="checkbox"/> Information Disclosure <input type="checkbox"/> Copies of IDS Statement (IDS)/PTO-1449 Citations 13. <input type="checkbox"/> Preliminary Amendment 14. <input checked="" type="checkbox"/> Return Receipt Postcard (MPEP 503) <small>(Should be specifically itemized)</small> 15. <input type="checkbox"/> Certified Copy of Priority Document(s) <small>(if foreign priority is claimed)</small> 16. <input type="checkbox"/> Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). <small>Applicant must attach form PTO/SB/35 or its equivalent.</small> 17. <input checked="" type="checkbox"/> Other: Certificate of Express Mailing (1 page) Check for \$40.00 for Assignment Recordation Only (1)	
18. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76: <input type="checkbox"/> Continuation <input type="checkbox"/> Divisional <input type="checkbox"/> Continuation-in-part (CIP) of prior application No.: _____ Prior application information: Examiner _____ Art Unit: _____ For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.			
<b>19. CORRESPONDENCE ADDRESS</b>			
<input checked="" type="checkbox"/> Customer Number: 38879 OR <input type="checkbox"/> Correspondence address below			
<b>Name</b> DARBY & DARBY P.C. Jamie L. Wiegand			
<b>Address</b> P.O. Box 5257			
<b>City</b>	New York	<b>State</b>	NY
<b>Country</b>	US	<b>Telephone</b>	(206) 262-8900
		<b>Fax</b>	(212) 753-6237
<b>Name (Print/Type)</b>	Jamie L. Wiegand		<b>Registration No. (Attorney/Agent)</b> 52,361
<b>Signature</b>			<b>Date</b> April 12, 2004

22387 U.S. PTO  
10/823378

041204

**FEE TRANSMITTAL  
for FY 2004**

Effective 10/01/2003, Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27**TOTAL AMOUNT OF PAYMENT (\$)** 40.00**Complete if Known**

Application Number	Not Yet Assigned
Filing Date	Concurrently Herewith
First Named Inventor	Adam Cain
Examiner Name	Not Yet Assigned
Art Unit	N/A
Attorney Docket No.	08212/0200353-USO

**METHOD OF PAYMENT (check all that apply)**☒ Check ☐ Credit Card ☐ Money Order ☐ Other ☐ None☐ Deposit Account:

Deposit Account Number

04-0100

Deposit Account Name

Darby &amp; Darby P.C.

The Director is authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☒ Credit any overpayments☐ Charge any additional fee(s) or any underpayment of fee(s)☒ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.**FEE CALCULATION****1. BASIC FILING FEE**

Large Entity		Small Entity		Fee Description	Fee Paid
Code	Fee (\$)	Code	Fee (\$)		
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

**SUBTOTAL (1) (\$)****2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE**

Total Claims	Extra Claims	Fee from below	Fee Paid
14	-20** =	x	0.00
3	-3** =	x	0.00
Multiple Dependent			

Large Entity		Small Entity		Fee Description	Fee Paid
Code	Fee (\$)	Code	Fee (\$)		
1202	18	2202	9	Claims in excess of 20	
1201	88	2201	43	Independent claims in excess of 3	
1203	280	2203	145	Multiple dependent claim, if not paid	
1204	88	2204	43	** Reissue independent claims over original patent	
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent	

**SUBTOTAL (2) (\$)** 0.00

\*\*or number previously paid, if greater; For Reissues, see above

**FEE CALCULATION (continued)****3. ADDITIONAL FEES**

Large Entity		Small Entity		Fee Description	Fee Paid
Code	Fee (\$)	Code	Fee (\$)		
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for <i>ex parte</i> reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	280	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	40.00
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify)

\*Reduced by Basic Filing Fee Paid

**SUBTOTAL (3) (\$)** 40.00**SUBMITTED BY**

Name (Print/Type) Jamie L. Wiegand

Signature

*Jamie L. Wiegand*Registration No.  
(Attorney/Agent)

52,361

(Complete if applicable)

Telephone (206) 262-8900

Date

April 12, 2004


{S:18212\0200353-USO\80006120.DOC #####}

## Certificate of Express Mailing Under 37 CFR 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Airbill No. EV398895255US in an envelope addressed to:

MS Patent Application  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

on April 12, 2004  
Date

  
\_\_\_\_\_  
Signature  
Jamie L. Wiegand  
\_\_\_\_\_  
Typed or printed name of person signing Certificate

Note: Each paper must have its own certificate of mailing, or this certificate must identify each submitted paper.

Check for \$40.00 for Assignment Recordation Only (1)  
Return Receipt Postcard (1)  
Certificate of Express Mailing (1 page)  
Utility Patent Application Transmittal (1 page)  
Fee Transmittal (1 page)  
Utility Application (Inc. Spec., Claims and Abstract) (17 pages)  
6 drawings (6 sheets)  
Oath or declaration (5 pages)  
Assignment Recordation Sheet (1 page)  
Assignment (3 pages)  
Application Data Sheet (3 pages)

**Application Filing Fee Not Being Paid At This Time**

{S:\8212\0200353-us0\80006118.DOC (11/11/04)}

**SYSTEM AND METHOD FOR ENABLING AUTHORIZATION OF A  
NETWORK DEVICE USING ATTRIBUTE CERTIFICATES**

**Field of the Invention**

5           The present invention relates to computer security, and in particular, to a system and method for authorizing access to a resource over a network using an attribute certificate.

**Background**

10           Earlier attempts to associate different authorization-related attributes to clients often relied on the client IP address as a means to identify the client. However, this technique proved not to be very effective, since the IP address of a network device may easily be changed. Furthermore, proliferation of Network Address Translation (NAT) devices and Virtual Private Networks (VPNs) makes it difficult for an access server to identify a particular client solely based on the client's IP address.

15           Commonly used Kerberos tickets provide a means for applications to share a cryptographically authenticated credential among several applications. However, Kerberos tickets only indicate that a particular user has successfully authenticated to a central network server, thereby establishing a single user session. Kerberos tickets do not convey user capabilities and they do not span multiple user  
20 sessions.

          The use of hardware tokens for authentication addresses a related need. A hardware token allows a user to prove its identity as well as its possession of a particular physical object. In return, those proven assertions may lead to an expanded access right for a network service. However, a hardware token also does not provide a  
25 general means to convey user capabilities of the client.

          Thus, it is with respect to these considerations and others that the present invention has been made.

{S:\8212\0200353-us0\80002667.DOC [REDACTED] } 1

### **Brief Description of the Drawings**

Non-limiting and non-exhaustive embodiments of the present invention are described with reference to the following drawings. In the drawings, like reference numerals refer to like parts throughout the various figures unless otherwise specified.

5 For a better understanding of the present invention, reference will be made to the following Detailed Description of the Invention, which is to be read in association with the accompanying drawings, wherein:

FIGURE 1 illustrates one embodiment of an environment in which the invention operates;

10 FIGURE 2 illustrates a functional block diagram of one embodiment of a network device that may be configured to operate as a client;

FIGURE 3 illustrates a flow diagram generally showing one embodiment of a process for using an attribute certificate to authorize a client;

15 FIGURE 4 illustrates message flows involved in one embodiment of the present invention;

FIGURE 5 illustrates message flows involved in another embodiment of the present invention; and

FIGURE 6 illustrates message flows involved in yet another embodiment of the present invention.

### **Detailed Description of the Preferred Embodiment**

20 The present invention now will be described more fully hereinafter with reference to the accompanying drawings, which form a part hereof, and which show, by way of illustration, specific exemplary embodiments by which the invention may be practiced. This invention may, however, be embodied in many different forms and  
25 should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Among other things, the present invention may be embodied as methods or devices. Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely

{S:\8212\0200353-us0\80002667.DOC }2

software embodiment or an embodiment combining software and hardware aspects.  
The following detailed description is, therefore, not to be taken in a limiting sense.

The terms "comprising," "including," "containing," "having," and  
"characterized by," refers to an open-ended or inclusive transitional construct and does  
5 not exclude additional, unrecited elements, or method steps. For example, a  
combination that comprises A and B elements, also reads on a combination of A, B, and  
C elements.

The meaning of "a," "an," and "the" include plural references. The  
meaning of "in" includes "in" and "on." Additionally, a reference to the singular  
10 includes a reference to the plural unless otherwise stated or is inconsistent with the  
disclosure herein.

The term "or" is an inclusive "or" operator, and includes the term  
"and/or," unless the context clearly dictates otherwise.

The phrase "in one embodiment," as used herein does not necessarily  
15 refer to the same embodiment, although it may.

The term "based on" is not exclusive and provides for being based on  
additional factors not described, unless the context clearly dictates otherwise.

The term "flow" includes a flow of packets through a network. The term  
"connection" refers to a flow or flows of messages that typically share a common  
20 source and destination.

Briefly stated, the present invention is directed to a method and system  
for authorizing a network device using attribute certificates.

Different network access capabilities may be provided to a user  
depending on properties of the user and device used to access the network. The  
25 invention may provide a secure way for the user to demonstrate that it has been  
approved for access to the network. An Attribute Certificate (AC) may be a digitally  
signed assertion including information about capabilities, restrictions, and the like, of  
the user and/or the device used to access the network. If the Attribute Certificate is  
issued upon completion of an automated security scan of a client device, the AC may be  
30 employed to provide a secure way for the device to inform an access server of the client

{S:\8212\0200353-us0\80002667.DOC 100 0000 0000 0000 0000 0000 0000 0000 }3

automated security scan results at a later time. If the AC is generated based on capabilities of the user, it provides the access server secure information needed to make network resources available to the user, based on the AC.

5 The AC may be issued to a user, which may present it to the access server from different client network devices. The AC may also be issued to a client network device, through which different users may access the same resource.

#### Illustrative Operating Environment

10 FIGURE 1 illustrates one embodiment of an environment in which a system may operate. Not all the components may be required to practice the invention, and variations in the arrangement and type of the components may be made without departing from the spirit or scope of the invention.

As shown in the figure, system 100 includes Local Area Network / Wide Area Network (LAN/WAN) 104, client 102, access server 106, attribute authority 108,  
15 and attribute repository 110. Client 102 and access server 106 are in communication over LAN/WAN 104. Access server 106 is in further communication with attribute authority 108 and attribute repository 110. Attribute authority 108 and attribute repository 110 are also in communication with each other.

LAN/WAN 104 is enabled to employ any form of computer readable  
20 media for communicating information from one electronic device to another. In addition, LAN/WAN 104 may include the Internet in addition to local area networks, wide area networks, direct channels, such as through a universal serial bus (USB) port, other forms of computer-readable media, and any combination thereof. On an interconnected set of LANs, including those based on differing architectures and  
25 protocols, a router acts as a link between LAN's, enabling messages to be sent from one to another. Also, communication links within LANs typically include twisted pair or coaxial cable, while communication links between networks may utilize analog telephone lines, full or fractional dedicated digital lines including T1, T2, T3, and T4, Integrated Services Digital Networks (ISDNs), Digital Subscriber Lines (DSLs),  
30 wireless links including satellite links, or other communications links known to those

{S:\8212\0200353-us0\80002667.DOC 0020 001 002 003 004 005 006 007 008 009 010 011 012 013 014 015 016 017 018 019 020 021 022 023 024 025 026 027 028 029 030 031 032 033 034 035 036 037 038 039 040 041 042 043 044 045 046 047 048 049 050 051 052 053 054 055 056 057 058 059 060 061 062 063 064 065 066 067 068 069 070 071 072 073 074 075 076 077 078 079 080 081 082 083 084 085 086 087 088 089 090 091 092 093 094 095 096 097 098 099 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 2494 2495 2496 2497 2498 2499 2500 2501 2502 2503 2504 2505 2506 2507 2508 2509 2510 2511 2512 2513 2514 2515 2516 2517 2518 2519 2520 2521 2522 2523 2524 2525 2526 2527



skilled in the art. Furthermore, remote computers and other related electronic devices may be remotely connected to either LANs or WANs via a modem and temporary telephone link. In essence LAN/WAN 104 may include any communication mechanism by which information may travel between network devices, such as client  
5 102 and access server 106.

Client 102 may be any network device capable of communicating over a network, such as LAN/WAN 104, to access server 106, and the like. The set of such devices may include devices that typically connect using a wired communications medium such as personal computers, multiprocessor systems, microprocessor-based or  
10 programmable consumer electronics, network PCs, and the like, that are configured to operate as a network device. The set of such devices may also include devices that typically connect using a wireless communications medium such as cell phones, smart phones, pagers, walkie talkies, radio frequency (RF) devices, infrared (IR) devices, CBs, integrated devices combining one or more of the preceding devices, and the like,  
15 that are configured as a network appliance. Alternatively, client 102 may be any device that is capable of connecting using a wired or wireless communication medium such as a PDA, POCKET PC, wearable computer, and any other device that is equipped to communicate over a wired and/or wireless communication medium, operating as a network device. As such client 102 may be configured to operate as a web server,  
20 cache server, file server, router, file storage device, gateway, switch, bridge, firewall, proxy, and the like.

Access server 106 may include any computing device or devices capable to provide authorization to a resource over LAN/WAN 104. Devices seeking access to the resource over the network, such as client 102 may be authorized by access server  
25 106 using an attribute certificate. Devices that may operate as access server 106 include, but are not limited to, personal computers, desktop computers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, web servers, cache servers, file servers, routers, gateways, switches, bridges, firewalls, proxies, and the like. The resource over the network may be any network service  
30 available to network devices connected to the network, such as client 102.

{S:\8212\0200353-us0\80002667.DOC [REDACTED] }5

Attribute authority 108 includes any computing device or devices capable to determine an attribute of a network device seeking authorization such as client 102. Attribute authority 108 may further include network devices that verify an attribute of a network device such as client 102. Attribute authority 108 may also be  
5 configured to operate as a web server, cache server, file server, router, file storage device, gateway, switch, bridge, firewall, proxy, and the like. In one embodiment attribute authority 108 and access server 106 may reside in one computing device.

Attribute repository 110 may include any computing device or devices capable of receiving an attribute certificate from access server 106, attribute authority  
10 108, and the like, and maintaining the attribute certificate ready for distribution. Devices that may operate as attribute repository 110 include, but are not limited to, personal computers, desktop computers, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, servers, and the like. Attribute repository 110 may also include a web service, an FTP service, an LDAP service, and  
15 the like, configured to manage the attribute certificate, and related information. In one embodiment, attribute repository 110 may include a storage structure for maintaining trust information, such as public keys, signatures, access control lists, revocation lists, and the like. Attribute repository 110 may include subscription information, observer mechanisms, and the like, that enable a network device, such as access server 106, and  
20 the like, to monitor an availability of the attribute certificate, and associated information.

Although not shown, attribute authority 108 and attribute repository 110 may also be in direct communication with client 102.

FIGURE 2 illustrates a functional block diagram of one embodiment of  
25 network device 200 in which the present invention may be practiced. Network device 200 provides one embodiment for access server 106 of FIGURE 1. It will be appreciated that not all components of network device 200 are illustrated, and that network device 200 may include more or less components than those shown in the figure. Network device 200 may operate, for example, as a personal computer, a  
30 desktop computer, a multiprocessor system, a microprocessor-based or programmable

{S:\8212\0200353-us0\80002667.DOC [REDACTED] }6

consumer electronic, a network PC, a web server, a cache server, a file server, a router, a gateway, a switch, a bridge, a firewall, a proxy, and the like. The communications may take place over a network, such as LAN/WAN 104 in FIGURE 1, the Internet, or some other communications network.

5                   As illustrated in FIGURE 2, network device 200 includes central processing unit (CPU) 212, video display adapter 214, read only memory (ROM) 232, random access memory (RAM) 216, hard disk drive 228, input/output interface (I/O) 224, a CD-ROM/DVD-ROM drive 226, and a network interface unit 210 interconnected via a bus 222.

10                   RAM 216, ROM 232, CD-ROM/DVD-ROM drive 226, and hard disk drive 228 are computer storage media, which may include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules or other data. Examples of computer storage media include RAM, ROM,  
15                   EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium that can store the information and that can be accessed by a computing device.

                  Network interface unit 210 is constructed for use with various  
20                   communication protocols including the TCP/IP and UDP/IP protocol. Network interface unit 210 may include or interface with circuitry and components for transmitting packets, and the like, over a wired and/or wireless communications medium. Network interface unit 210 is sometimes referred to as a transceiver, Network Interface Card (NIC), and the like. Network device 200 may also include an I/O  
25                   interface 224 for communicating with external devices or users.

                  RAM 216 is generally interconnected with ROM 232 and one or more permanent mass storage devices, such as hard disk drive 228. RAM 216 stores operating system 220 for controlling the operation of network device 200. The operating system 220 may comprise an operating system such as UNIX, LINUX™,  
30                   Windows™, and the like.

{S:\8212\0200353-us0\80002667.DOC [REDACTED] }7

In one embodiment, RAM 216 stores program code for application software 250, authorization protocol 240, and Attribute Certificate (AC) evaluation protocol 242, and the like, for performing authorization functions of network device 200. Application software 250 may include any computer program. Authorization  
5 protocol 240 is directed to controlling access to a network resource as described in FIGURE 3. AC evaluation protocol 242 may be a complementary protocol that enables the authorization protocol 240 to evaluate an attribute of a network device, such as client 102 of FIGURE 1, desiring access to the resource over the network. The attribute may be based, in part, on a capability of client 102, a condition to be satisfied for  
10 another attribute to be valid, a result of an automated security scan, and the like.

#### General Operation

FIGURE 3 illustrates a flow diagram generally showing process 300 for authorizing a network device using attribute certificates, according to one embodiment  
15 of the invention. Process 300 may, for example, be implemented in access server 106 of FIGURE 1.

As shown in FIGURE 3, process 300 begins, after a start block, at block 302, where an attribute of the network device desiring authorization, such as client 102 of FIGURE 1, is determined. The attribute may be based, in part, on a capability or  
20 characteristic of the network device. For example, the network device may be a laptop issued to a particular user, and the like. In this example, the attribute may be based, in part, on the status of security software running on the network device, and the like.

The attribute, determined at block 302, may also be based, in part, on a condition to be satisfied for another attribute to be valid. In the above example, the  
25 primary attribute may be the assertion that the network device has an anti-virus software installed. The other attribute may be based, in part, on a condition that the anti-virus software is running on the network device, and the antivirus software is configured with virus definitions that are no more than 5 days old, as a further example.

In another embodiment, the attribute, determined at block 302 may  
30 further be based, in part, on a status of the network device desiring authorization, such

{S:\8212\0200353-us0\80002667.DOC [REDACTED] }8

as a result of an automated security scan. For security reasons, an automated security scan of the network device may be performed and the result associated with the AC. Associating an automated security scan with the AC may eliminate the need to perform repeated automated security scans every time the network device requests authorization, since the AC may provide evidence of a recent automated security scan. Upon determination of the attribute to be associated with the AC, process 300 proceeds to block 304.

At block 304, the AC is generated based, in part, on the attribute determined at block 302. The AC may be generated by the device performing the authorization, such as access server 106 of FIGURE 1, the network device itself, a third party network device, such as the attribute authority 108 of FIGURE 1, and the like.

Processing then proceeds to block 306 of FIGURE 3, where the AC is stored. The storage may also be performed by the device performing the authorization, such as access server 106 of FIGURE 1, the network device itself, a third party network device, such as the attribute authority 108 of FIGURE 1, and the like. Upon completion of block 306, process 300 may wait until a request for authorization is received at block 308.

At block 308, the network device presents the authorizing device with a request for authorization. Although not shown, block 308 may include actions by the authorizing device including, but not limited to, retrieving the AC from the network device, a storage device, an external storage database, and the like.

Process 300 flows to block 310, where a decision is made, to determine whether the network device is authenticated for connection to the network. If authentication is verified, processing proceeds to decision block 312. If authentication is not verified, processing proceeds to block 316, where communication is terminated. Processing may then return to a calling process to perform other actions.

At block 312, the validity of the AC is determined. In determining the validity of the AC a number of factors may be used including, but not limited to, valid date range of the AC, device identifier recorded in the AC, digital signature, and the like. If the AC is valid, process 300 proceeds to block 314, where the network device is

{S:\8212\0200353-us0\80002667.DOC }9

authorized. If the AC is not valid, processing proceeds to block 316, where communication is terminated. Processing may then return to a calling process to perform other actions.

It will be understood that each block of the flowchart illustrations discussed above, and combinations of blocks in the flowchart illustrations above, can be implemented by computer program instructions. These program instructions may be provided to a processor to produce a machine, such that the instructions, which execute on the processor, create means for implementing the actions specified in the flowchart block or blocks. The computer program instructions may be executed by a processor to cause a series of operational steps to be performed by the processor to produce a computer-implemented process such that the instructions, which execute on the processor, provide steps for implementing the actions specified in the flowchart block or blocks.

Although the invention is described in terms of communication between a network device and an access server, the invention is not so limited. For example, the communication may be between virtually any resource, including but not limited to multiple clients, multiple servers, and any other device, without departing from the scope of the invention.

Accordingly, blocks of the flowchart illustrations support combinations of means for performing the specified actions, combinations of steps for performing the specified actions and program instruction means for performing the specified actions. It will also be understood that each block of the flowchart illustrations, and combinations of blocks in the flowchart illustrations, can be implemented by special purpose hardware-based systems, which perform the specified actions or steps, or combinations of special purpose hardware and computer instructions.

#### Illustrative Embodiments

FIGURE 4 illustrates one embodiment of a message flow diagram for a system similar to the system shown in FIGURE 1. As shown in the diagram, message flow 400 includes network resource 402, attribute repository 404, access server 406,

{S:\8212\0200353-us0\80002667.DOC [REDACTED] } 10

and client 408 across the top. Client 408 and access server 406 may operate substantially similar to client 102 and access server 106, respectively, of FIGURE 1. Time may be viewed as flowing downward in the figure.

As shown in FIGURE 4, the message flows are divided into two groups separated by timeline 410. The first group comprises message flows involved in generating and storing an AC. This process may be repeated, if client 408 desires to store a certificate with a new access server, the stored AC is no longer valid for any of a variety of reasons, and the like. The process begins with access server 406 determining an attribute of client 408 to be associated with the AC. The attribute may be based, in part, on a capability of client 408. For example, client 408 may be a network device used by a user possessing temporary approval to utilize print services provided by a network resource. In this example, access server 406 may verify the printing capability approval for the network resource as the attribute to be associated with the AC.

Access server 406 may then generate the AC based, in part, on the attribute determined above. Following generation of the AC, access server 406 may send the AC to attribute repository 404, where the AC is stored.

The authorization process, as shown below timeline 410, in FIGURE 4, is typically started by receiving of a request for authorization from client 408. Upon receiving the request for authorization from client 408, access server 406 authenticates client 408. Authentication may be based on a login password, a digital certificate, a biometric parameter, and the like.

Upon authentication, access server 406 requests the AC from attribute repository 404. Attribute repository 404 sends the AC to access server 406, which verifies the AC's validity. The validity of the AC may be verified based, in part, on any one of a number of factors including, but not limited to, the date range of the AC, digital signature on the AC, comparison of the identity listed in the AC with the authenticated identity of client 408, and the like.

If the AC is valid, access server 406 authorizes client 408 based, in part, on the attribute associated with the AC. Further using the example above, the

{S:\8212\0200353-us0\80002667.DOC [REDACTED] } 11

authorization provides client 408 with access to printing capabilities of network resource 402 based, in part, on the attribute associated with the AC.

FIGURE 5 illustrates a message flow diagram for a network system in accordance with another embodiment of the present invention. As shown in the diagram, message flow 500 includes network resource 502, access server 504, and client 506 across the top. Client 506 and access server 504 may operate substantially similar to client 102 and access server 106, respectively, of FIGURE 1. Time may be viewed as flowing downward in the figure.

As shown in FIGURE 5, the message flows are divided into two groups separated by timeline 508. The first group comprises message flows involved in generating and storing an AC. The first part of the process is substantially similar to the first process described in FIGURE 4, above timeline 410. One difference between the two processes is access server 504 sends the AC to client 506 instead of an attribute repository, and client 506 stores the AC.

The authorization process, as shown below timeline 508, in FIGURE 5, is typically started by receiving of a request for authorization from client 506. Upon receiving the request for authorization from client 506, access server 504 authenticates client 506. Authentication may be based on a login password, a digital certificate, a biometric parameter, and the like.

Upon authentication, access server 504 verifies that the client is in possession of a valid AC. The validity of the AC may be verified based, in part, on any one of a number of factors including, but not limited to, the date range of the AC, digital signature on the AC, comparison of the identity listed in the AC with the authenticated identity of client 506, and the like.

If the AC is valid, access server 504 authorizes client 506 based, in part, on the attribute associated with the AC. Using the example described in FIGURE 4 above, the authorization provides client 506 with access to printing capabilities of network resource 502 based, in part, on the attribute associated with the AC.

FIGURE 6 illustrates a message flow diagram for a network system in accordance with a further embodiment of the present invention. As shown in the

{S:\8212\0200353-us0\80002667.DOC } 12



diagram, message flow 600 includes access server 602, client 604, and attribute authority 606 across the top. Client 604 and access server 602 may operate substantially similar to client 102 and access server 106, respectively, of FIGURE 1. Time may be viewed as flowing downward in the figure.

5                   As shown in FIGURE 6, the message flows are divided into two groups separated by timeline 608. The first group comprises message flows involved in generating and storing an AC. The process begins with an automated security scan of client 604 performed by attribute authority 606. Attribute authority 606 generates the AC based, in part, on a result of the automated security scan of client 604, and stores the  
10   AC.

                  The authorization process, as shown below timeline 608, in FIGURE 6, is typically started by receiving of a request for authorization from client 604. Upon receiving the request for authorization from client 604, access server 602 authenticates client 604. Authentication may be based on a login password, a digital certificate, a  
15   biometric parameter, and the like.

                  Upon authentication, access server 602 requests the AC from attribute authority 606. Attribute authority 606 send the AC to access server 602, which verifies the validity of the AC. The validity of the AC may be verified based, in part, on any one of a number of factors including, but not limited to, the date range of the AC, digital  
20   signature on the AC, and the like.

                  If the AC is valid, access server 602 authorizes client 604 based, in part, on the attribute associated with the AC. In this embodiment, the authorization provides client 604 with access to network resources.

                  The above specification, examples, and data provide a complete  
25   description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

**WE CLAIM:**

1. A method for authorizing a network device, comprising:  
determining an attribute based, in part, on a capability of the network device;  
generating an attribute certificate based, in part, on the attribute;  
storing the attribute certificate including the attribute; and  
if the attribute certificate is valid, authorizing access to a resource over a network based, in part, on the attribute associated with the attribute certificate.
2. The method of Claim 1, wherein the attribute is further determined based, in part, on an automated security scan of the network device.
3. The method of Claim 1, wherein the attribute is further determined based, in part, on a condition to be satisfied.
4. The method of Claim 1, wherein the attribute is further associated with a group of network devices.
5. The method of Claim 1, wherein the attribute is further associated with a group of users.
6. The method of Claim 1, wherein the attribute certificate is generated by at least one of the network device, an access server, and an attribute authority.
7. The method of Claim 1, wherein the attribute certificate is stored in at least one of the network device, and an attribute repository.
8. The method of Claim 7, wherein the attribute certificate is provided to an access server through the use of at least one of a cookie, a program, and a manual upload.

{S:\8212\0200353-us0\80002667.DOC [REDACTED] } 14



{S:\8212\0200353-us0\80002667.DOC 10/12/07 10:17:17 AM } 16

### Abstract

Methods and devices are directed to authorizing a network device to a resource over a network. An access server determines based, in part, on an attribute of the network device associated with the attribute certificate, whether the network device may be authorized access to the resource over the network. The attribute may be associated with a capability granted to the network device, a condition to be satisfied for the attribute to be valid, and the like. The attribute may belong to a group of network devices, or one or more users accessing the network through the network device. In one embodiment, the attribute certificate may be provided based on an automated security scan of the network device. In another embodiment, the access server may make the attribute available to a network resource associated with the access server.

Customer No. 38879

{S:\8212\0200353-us0\80002667.DOC 11/11/01 11:11:11 AM } 17

## DECLARATION FOR PATENT APPLICATION

**EARLIEST FOREIGN APPLICATION(S), IF ANY FILED WITHIN 12 MONTHS  
(6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION**

Application Number	Country	Date of Filing	Priority Claimed Under 35 USC 119
			___ Yes No ___
			___ Yes No ___
			___ Yes No ___

**ALL FOREIGN APPLICATION(S), IF ANY FILED MORE THAN 12 MONTHS  
(6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION**

Application Number	Country	Date of Filing

**CLAIM FOR BENEFIT OF EARLIER U.S. PROVISIONAL APPLICATIONS**

I hereby claim priority benefits under Title 35, United States Code §119(e), of any United States provisional patent application(s) listed below:

☒ no such U.S. provisional applications have been filed.

☐ such U.S. provisional application have been filed as follows:

Application Number	Date of Filing	Priority Claimed Under 35 USC 119
		___ Yes No ___
		___ Yes No ___
		___ Yes No ___

**CLAIM FOR BENEFIT OF EARLIER U.S./PCT APPLICATION(S)**

I hereby claim the benefit under Title 35, United States Code, §120 of the United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose all information that is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56 which became available to me between the filing date of the prior application and the national or PCT international filing date of this application:

{S:\8212\0200353-us0\80002608.DOC [REDACTED]}

☒ no such U.S./PCT applications have been filed.

☐ such U.S./PCT application have been filed as follows:

Application Number	Date of Filing	Status (Patented/Pending/Abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the practitioners under Customer Number

38879

all of **Darby & Darby P.C.**, P.O. Box 5257, New York, New York 10150-5257, jointly, and each of them severally, my attorneys at law/patent agent(s), with full power of substitution, delegation and revocation, to prosecute this application, to make alterations and amendments therein, to receive the patent, and to transact all business in the U. S. Patent and Trademark Office connected therewith.

Please mail all correspondence to Jamie L. Wiegand, whose address is:


**Darby & Darby P.C.**  
P.O. Box 5257  
New York, New York 10150-5257

Please direct telephone calls to: Jamie L. Wiegand at (206) 262-8915.

Please direct facsimiles to: (212) 753-6237




Attorney Docket No.: 08212/0200353-US0

Full name of third inventor, if any <b>Adam Cain</b>	
Third inventor's signature 	Date <b>3/7/04</b>
Residence <b>Madison, Wisconsin</b>	
Citizenship <b>US</b>	
Mailing Address  <b>461 N. Few St. Madison, Wisconsin 53703</b>	

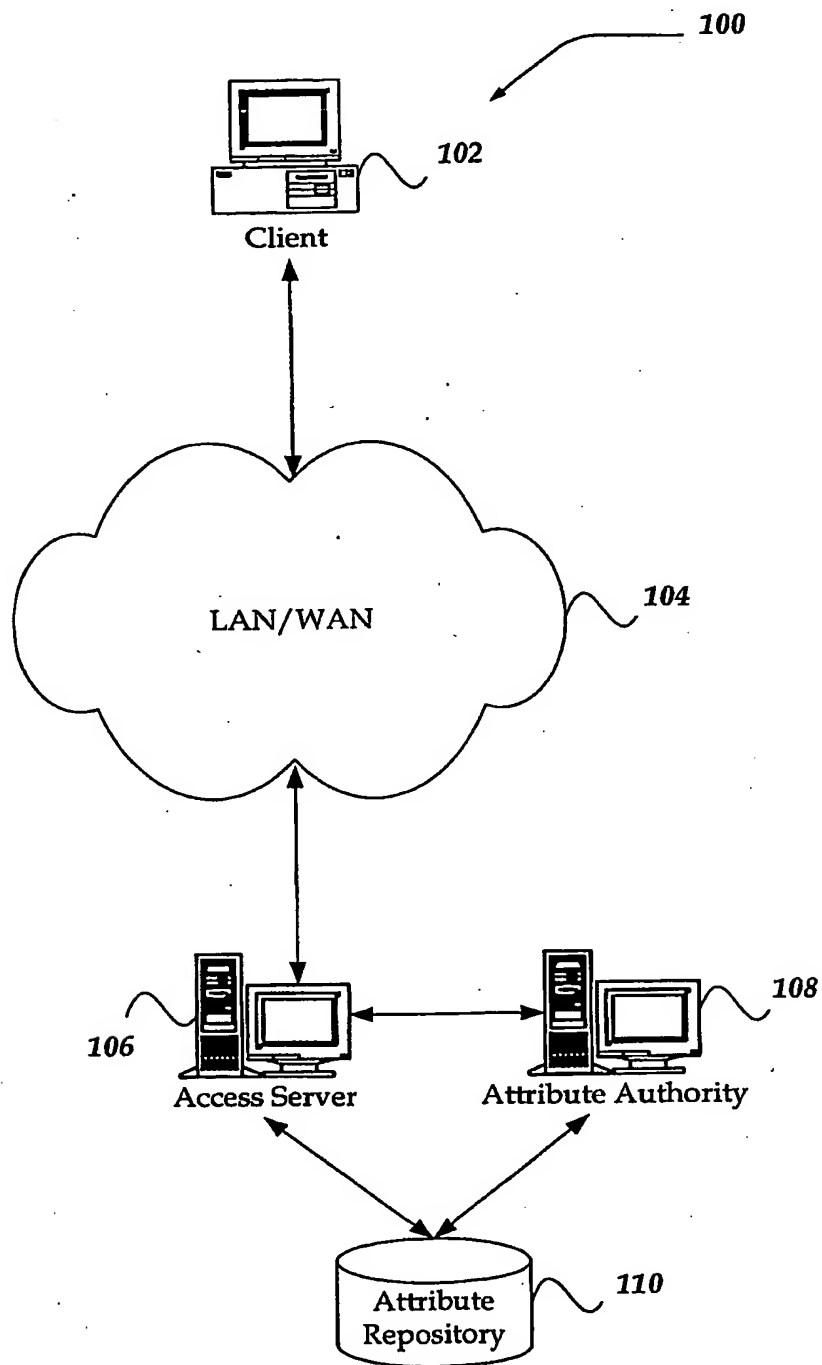
Full name of sole or first inventor <b>Craig R. Watkins</b>	
Sole or first inventor's signature	Date
Residence <b>State College, Pennsylvania</b>	
Citizenship <b>US</b>	
Mailing Address  <b>1883 Huntington Lane State College, Pennsylvania 16803-3346</b>	

Full name of second inventor, if any <b>Jeremey Barrett</b>	
Second inventor's signature	Date
Residence <b>Sugar Land, Texas</b>	
Citizenship <b>US</b>	
Mailing Address  <b>3330 Big Horn Ct. Sugar Land, Texas 77478</b>	

Full name of third inventor, if any <b>Adam Cain</b>	
Third inventor's signature	Date
Residence <b>Madison, Wisconsin</b>	
Citizenship <b>US</b>	
Mailing Address  <b>461 N. Few St. Madison, Wisconsin 53703</b>	

Full name of sole or first inventor <b>Craig R. Watkins</b>	
Sole or first inventor's signature 	Date <b>20 Feb 2004</b>
Residence <b>State College, Pennsylvania</b>	
Citizenship <b>US</b>	
Mailing Address  <b>1883 Huntington Lane State College, Pennsylvania 16803-3346</b>	

Full name of second inventor, if any <b>Jeremey Barrett</b>	
Second inventor's signature	Date
Residence <b>Sugar Land, Texas</b>	
Citizenship <b>US</b>	
Mailing Address  <b>3330 Big Horn Ct. Sugar Land, Texas 77478</b>	



**FIG. 1**

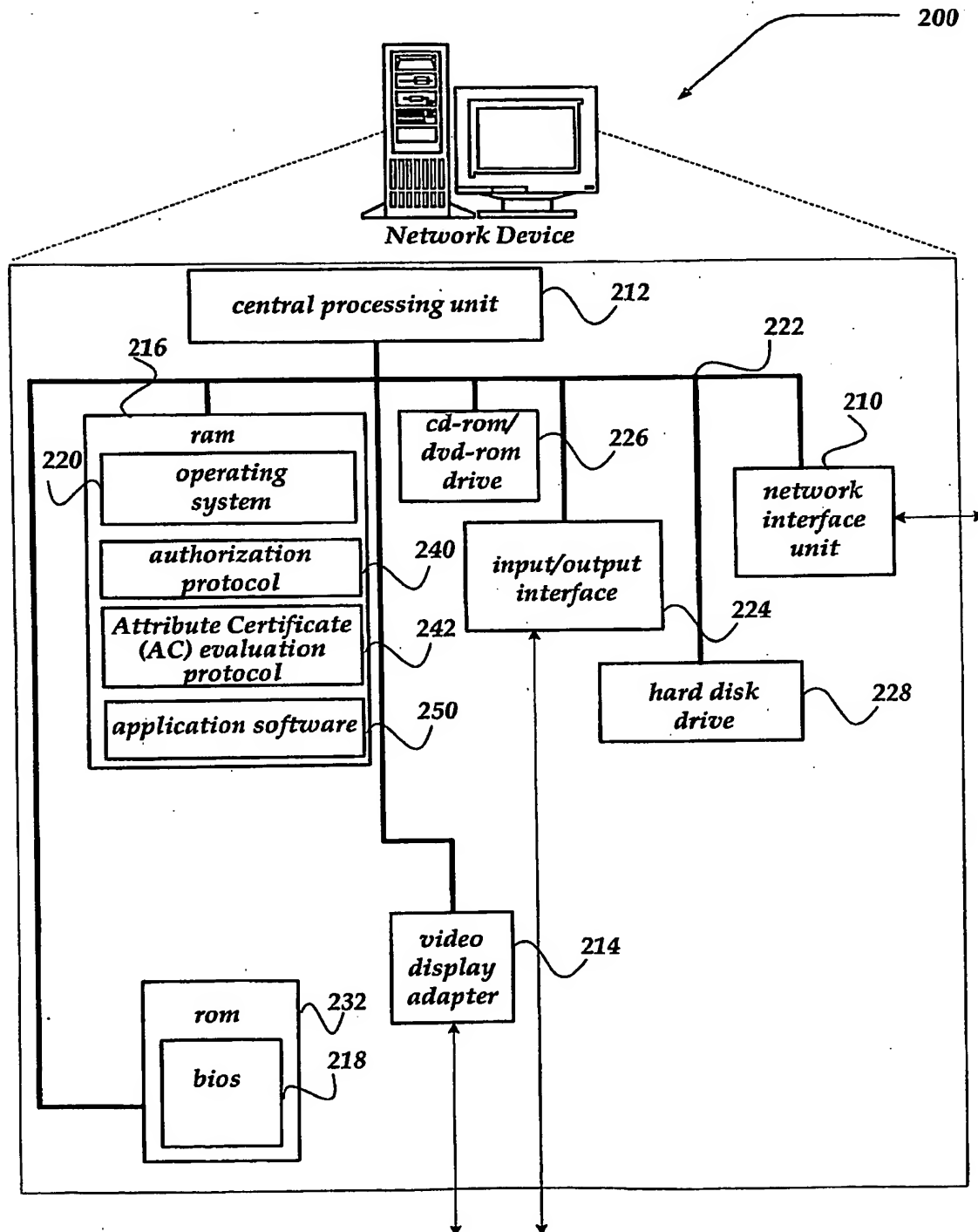


FIG. 2

Title:

SYSTEM AND METHOD FOR ENABLING AUTHORIZATION  
OF A NETWORK DEVICE USING ATTRIBUTE CERTIFICATES

Inventors:

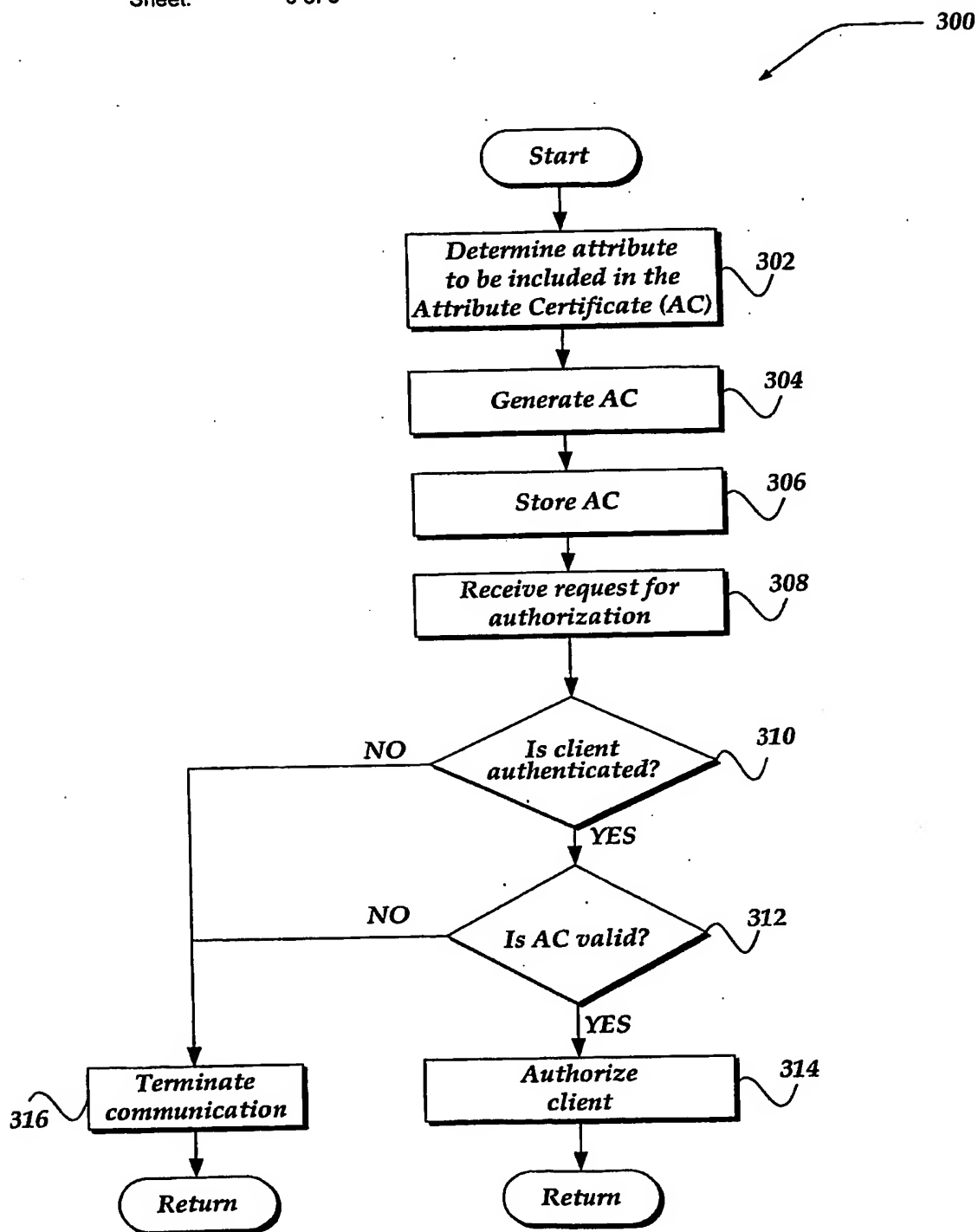
Adam Cain, et al.

Docket No.:

08212/0200353-US0

Sheet:

3 of 6



**FIG. 3**

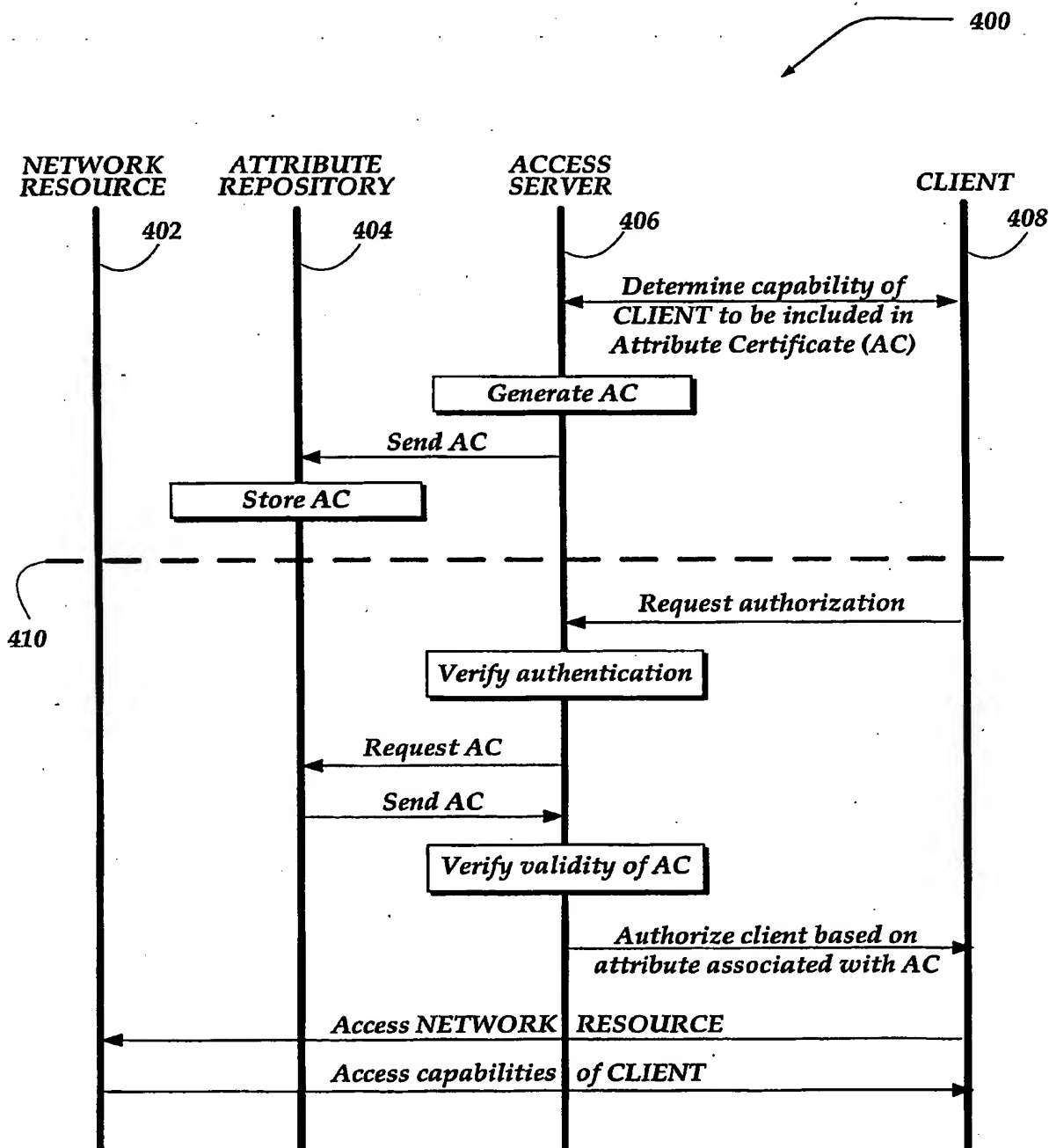


FIG. 4

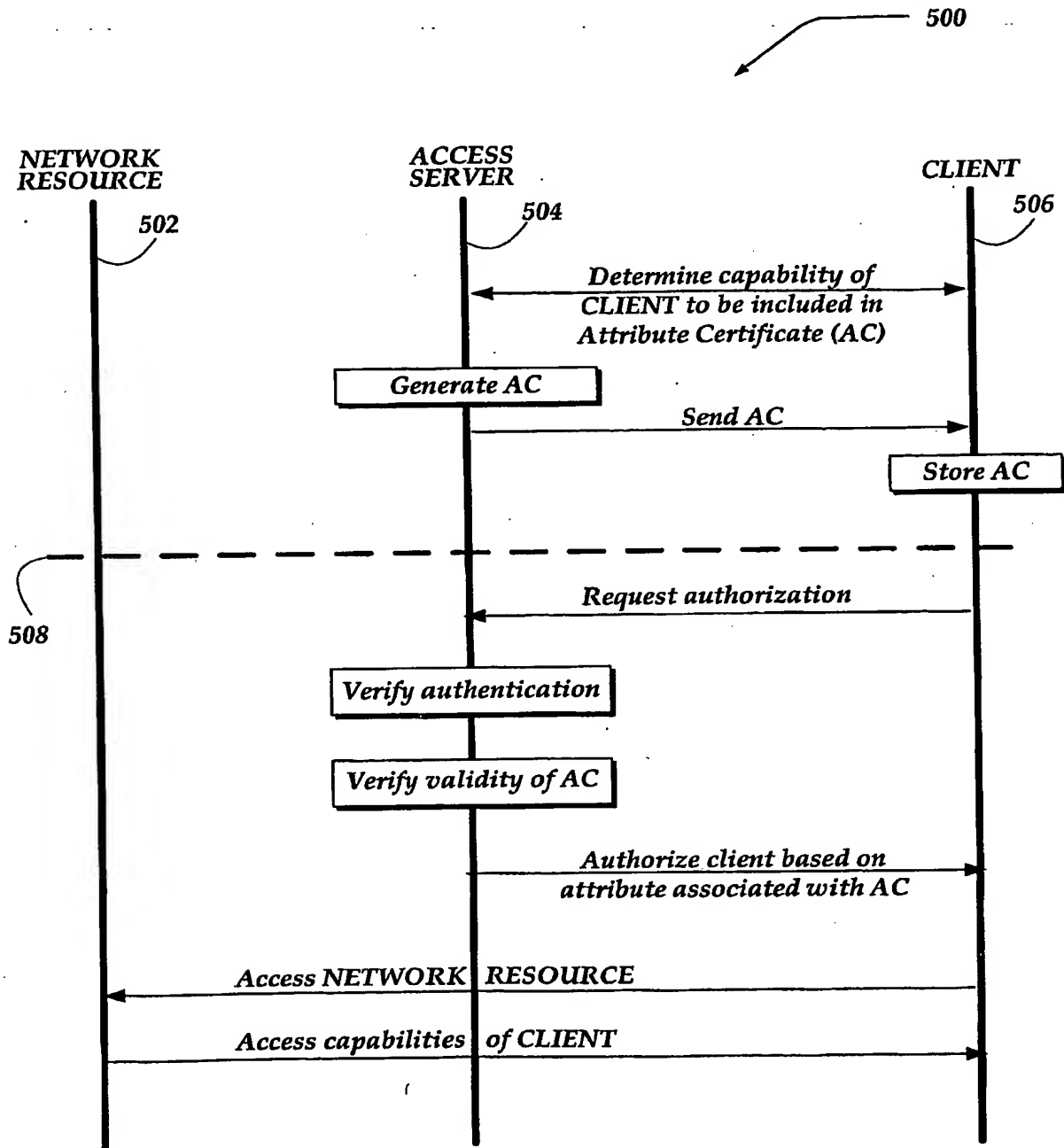


FIG. 5

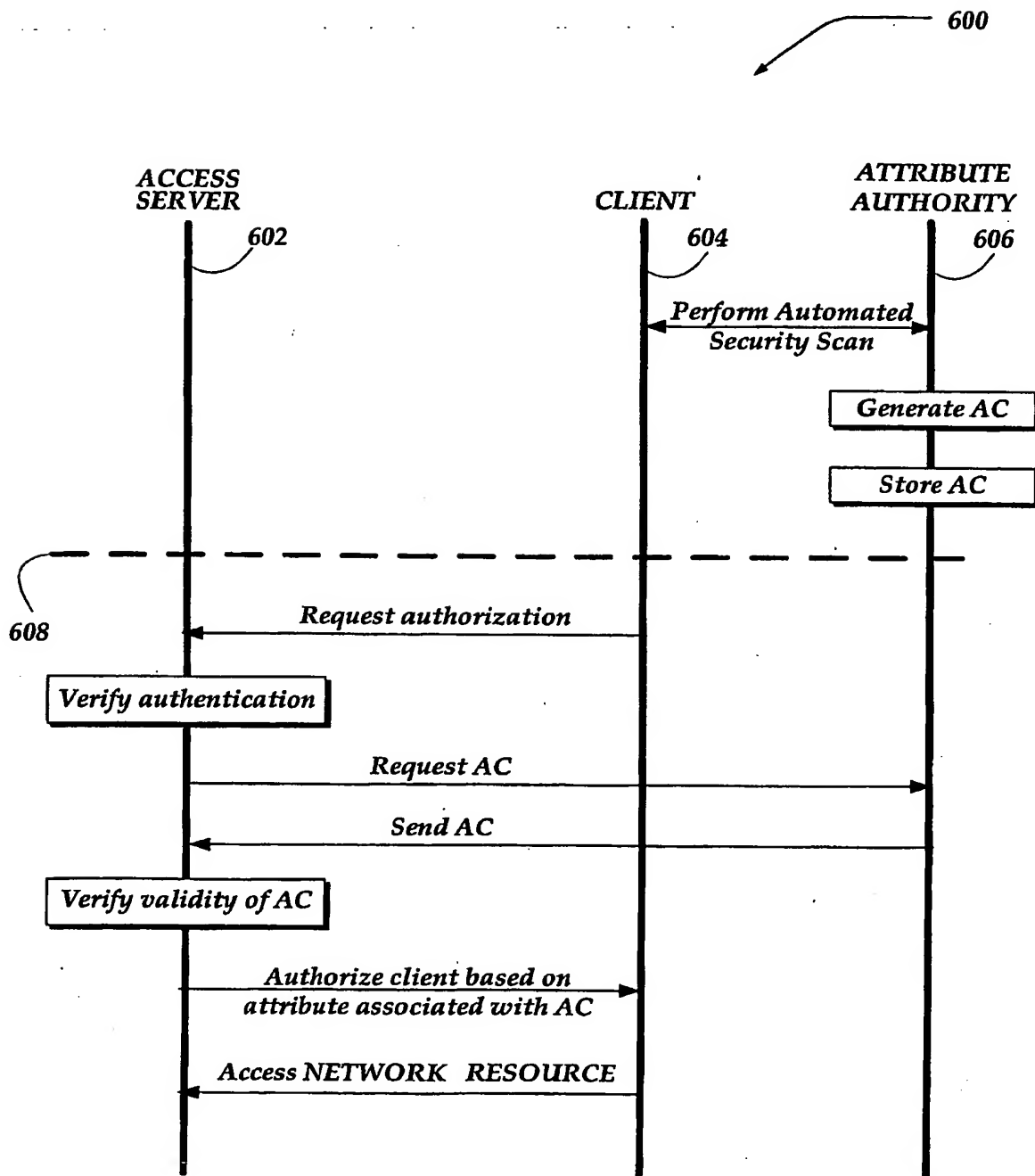


FIG. 6



## **Application Data Sheet**

### **Application Information**

Application Type::	Regular
Subject Matter::	Utility
Suggested Group Art Unit::	N/A
CD-ROM or CD-R?::	None
Sequence submission?::	None
Computer Readable Form (CRF)?::	No
Title::	SYSTEM AND METHOD FOR ENABLING AUTHORIZATION OF A NETWORK DEVICE USING ATTRIBUTE CERTIFICATES
Attorney Docket Number::	08212/0200353-US0
Request for Early Publication?::	No
Request for Non-Publication?::	No
Total Drawing Sheets::	6
Small Entity?::	No
Petition included?::	No
Secrecy Order in Parent Appl.?::	No

### **Applicant Information**

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Status::	Full Capacity
Given Name::	Adam
Family Name::	Cain
City of Residence::	Madison
State or Province of Residence::	WI
Country of Residence::	US
Street of mailing address::	461 N. Few St.
City of mailing address::	Madison

State or Province of mailing address:: WI  
Postal or Zip Code of mailing address:: 53703

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: US  
Status:: Full Capacity  
Given Name:: Craig  
Middle Name:: R.  
Family Name:: Watkins  
City of Residence:: State College  
State or Province of Residence:: PA  
Country of Residence:: US  
Street of mailing address:: 1883 Huntington Lane  
City of mailing address:: State College  
State or Province of mailing address:: PA  
Postal or Zip Code of mailing address:: 16803-3346

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: US  
Status:: Full Capacity  
Given Name:: Jeremey  
Family Name:: Barrett  
City of Residence:: Sugar Land  
State or Province of Residence:: TX  
Country of Residence:: US  
Street of mailing address:: 3330 Big Horn Ct.  
City of mailing address:: Sugar Land  
State or Province of mailing address:: TX  
Postal or Zip Code of mailing address:: 77478

#### **Correspondence Information**

Correspondence Customer Number:: 38879

**Representative Information**

Representative Customer Number:: 38879

**Assignee Information**

Assignee name:: Nokia, Inc.  
Street of mailing address:: 6000 Connection Drive  
City of mailing address:: Irving  
State or Province of mailing address:: TX  
Postal or Zip Code of mailing address:: 75039